IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Thomas E. Tahan	§	Group Art Unit: 2137 Examiner: Michael J. Pyzocha Atty. Dkt.: 5181-75900
Serial No.: 09/923,588	§	
Filed: August 7, 2001	§	
For: CONTROLLED INFORMATION FLOW BETWEEN COMMUNITIES VIA A FIREWALL	§	

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Dear Sir or Madam:

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request. This request is being filed with a notice of appeal. The review is requested for the reason(s) below. Applicant is in receipt of the Final Office Action mailed July 14, 2006 and Advisory Action dated October 26, 2006. Claims 1-4, 6, 8-21, 23, 25-38, 40, and 42-51 remain pending in the application. Reconsideration of the present case is earnestly requested in light of the following remarks. Claims 1-2, 6, 8, 10, 12, 15-16, 18-19, 23, 25, 27, 29, 32-33, 35-36, 40, 42, 44, 46, and 49-50 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Bots, U.S. Patent No. 6,226,748 (hereinafter "Bots"). Claims 3, 11, 20, 28, 37, and 45 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bots in view of McNeill, U.S. Patent No. 6,167,052. Claims 4, 13, 21, 30, 38, and 47 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bots in view of Kidambi, U.S. Patent No. 6,424,626. Finally, claims 14, 17, 31, 34, 48, and 51 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bots in view of Kisor, U.S. Patent No. 6,266,773. The following clear errors in the Examiner's rejection are noted.

Claim 1 recites a method of controlling information flow through a firewall. Recited in the claim are a number of features including determining, discarding, and processing features. In addition, claim 1 specifically recites that the recited determining, discarding, and processing are performed within a single node of a network. Applicant submits at least these features are not disclosed by the cited art.

In the Final Office Action dated July 14, 2006, the examiner cites Bots as anticipating claim 1. With respect to the above features, the examiner cites a portion of Bots which discloses a first virtual private network (VPN) unit 250 coupled via Internet (or other unsecured network space) to another virtual private network unit 252. The examiner then states that the disclosure of a VPN unit coupled via Internet to another VPN unit are equivalent to a single firewall node of a network as recited in the claim. In particular, the examiner states on page 7 of the Final Office Action:

> "Bots discloses a network security system in which computer terminals in disparate networks may wish to communicate (e.g. device 201 in LAN A may wish to communicate with device 211 in LAN B). In order to accomplish this task in a secure fashion, Bots implements a unique firewall comprising Virtual Private Network Units (VPNUs). Thus, device 201 in LAN A may pass a packet via a router through the firewall, which may comprise VPNUs 250 and 252. If the firewall authenticates the packet, it is output to device 211. Examiner agrees that the two VPNUs are two units. However, the two VPNUs are acting as part of a single firewall entity. Without language precluding the foregoing 15 entity from meeting "a node", the claims are given their broadest reasonable interpretation (see MPEP 2111)."

In the above, the examiner equates the computer terminals in disparate networks communicating via virtual private network with a firewall node. However, Applicant submits a virtual private network is clearly not a single node of a network, and to equate the two is not a reasonable interpretation of "node of a network" as recited. Those skilled in the art have no difficulty in distinguishing a firewall node from a virtual private network. While not believed necessary, Applicant provides the following typical definitions of "node" from a variety of web based dictionaries:

Free Online Dictionary of Computing - An addressable device attached to a computer network

Netlingo - A device (even a printer) that is connected to a network. Every node has a unique network address, sometimes called a Data Link Control (DLC) address or Media Access Control (MAC) address.

Hutchinson Dictionary of Computers, Multimedia, and the Internet - Any device connected to a network, such as a router, a bridge, a hub, and a server.

Geek.com - One computer/machine or address on a network. If you managed a network with 10 printers, 50 servers, and 150 client machines, you could say you managed a network with 210 nodes.

LearnTheNet.com - A node is an addressable point on a network. A node can connect a computer system, a terminal, or various peripheral devices to the network. Each node on a network has a distinct name. On the Internet, a node is a host computer with a unique domain name and address that has been assigned to it by InterNIC.

Linktionary.com - A node is a network-connected device such as a workstation, a server, or a printer.

> Techweb.com - In a communications system, a node is a network junction or connection point. Every terminal, computer, hub and switch is a node.

Accordingly, Applicant does not agree with the examiner's contention that the virtual private network of Bots is a single node of a network as recited. As the examiner seeks to identify the various features of the claim as occurring partially in one VPN unit of a network and other features occurring in another VPN unit of a network, Applicant submits Bots clearly does not disclose the single node and the recited features are all performed within a single node of a network. For at least these reasons, claim 1 is patentably distinguishable from Bots and withdrawal of the rejections is requested. Each of independent claims 18 and 35 are patentably distinguishable for similar reasons.

Further, in an effort to equate various aspects of the claim to the disclosure of Bots, the examiner suggests Bots "implements a unique firewall comprising Virtual Private Network Units (VPNUs)". However, Applicant submits a firewall and a VPN are not the same, and <u>even the Bots reference itself does not agree with such a statement</u>. In contrast to the assertion of the examiner, Bots expressly states:

> "The overall architecture of the present invention is robust. It allows end users the convenience of proprietary data communications to take place over a public network space such as the Internet. The architecture of the present invention also allows a wide variety of compression, encryption and authentication technologies to be implemented, so long as the VPN units at each end of the transaction support the associated protocols. <u>The present invention is also capable of working in concert with traditional Internet security mechanisms such as corporate firewalls. A firewall might operate in series with the VPN unit at a given site, or, intelligently be configured in a single box with the VPN unit to provide parallel firewall and VPN unit security functions</u>." (Bots, col. 9, lines 13-25).

As seen from the above, Bots makes a clear distinction between a firewall on the one hand, and the disclosed VPN system. Therefore, even the reference itself disagrees with the characterizations of the reference provided by the examiner. Consequently, the examiner's effort to somehow equate a virtual private network with a firewall node are misplaced.

In addition to the above, even were one to accept the examiner's assertion that a pair of VPNUs communicating via a public unsecured network is equivalent to a single network node configured to act as a firewall, Bots fails to disclose all of the features of claims 1, 18, and 35. For example, claim 1 recites, in relevant part:

> "... matching said first data packet to a first rule of a plurality of rules of said firewall;
> comparing said first incoming PCS to a second incoming PCS specified by the first rule;

> changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS …"

Applicant submits that Bots fails to disclose "changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS", as is recited in claim 1. Rather, Bots discloses:

> "The particular packet processing algorithms to be used for VPN traffic may vary, so long as the lookup tables in both the sending and receiving VPN units identify the same compression, encryption and authentication rules and are capable of implementing and deimplementing them for members of the same group. It is to be understood that a single VPNU may serve multiple VPN groups and that particular addresses may be members of multiple groups. Thus, at step 340, when a packet is destined from one member of the VPN group to another, the packet is processed according to the compression, encryption and authentication rules identified in the VPNU tables for that particular VPN group." (Bots, Col. 7, lines 40-52).

Therefore, while Bots discloses processing steps of compression, encryption, and authentication, Bots fails to teach or suggest changing the VPN group. Compression, encryption, and authentication are well-known processes that do not change group membership. Accordingly, Applicant submits that Bots fails to teach "changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule," as is recited in claim 1.

In addition, claim 1 recites three comparisons: (1) detecting said first incoming PCS is not a subset of an interface community set (IFCS) of said interface, (2) comparing said first incoming PCS to a second incoming PCS specified by the first rule, and (3) comparing said outgoing PCS with a destination community set of said first data packet. Bots fails to teach or suggest all three comparisons as recited. In contrast to the above claimed features, Bots discloses:

> "At decision box 320, it is determined whether or not the source and destination addresses for the data packet are both members of the same VPN group. This determination may be made with reference to lookup tables that are maintained by the VPN units or reference to other memory mechanisms. This step may be thought of as member filtering for data packets being transmitted between the particular site and the VPN unit which services it." (Bots, Col. 7, lines 1-9).
>
> "At decision box 420, the inbound data packet is examined to determine if the source and destination addresses of the data packet are both members of the same VPN group. It is assumed that the lookup tables maintained by all of the VPN units are both consistent and coherent." (Bots, Col. 7, lines 60-65).

As may be seen from the above, Bots's method looks up the VPN group of the source address and the VPN group of the destination address and compares them to see if the two groups are the same. These steps are performed in both the transmitting VPNU and the receiving VPNU. Hence, Bots discloses, at most, two comparisons. Furthermore, since Bots does not disclose changing the source or destination address between the first VPNU and the second VPNU, and since Bots assumes that the lookup tables maintained by all of the VPN units are both consistent and coherent, Bots's second comparison is a repetition of the first comparison, i.e. it is a comparison of the source VPN group with the destination VPN group. In contrast, the three comparisons recited in claim 1 involve a first incoming PCS and an (IFCS), a first incoming PCS and a second incoming PCS, and an outgoing PCS and a destination community set. No two of these comparisons involve the same two community sets. Accordingly, Applicant submits that Bots fails to disclose more than one of the comparisons recited in claim 1.

Also, there are significant additional differences between the comparisons disclosed by Bots and the claimed features. For example, Bots compares the VPN group of the source address with the VPN group of the destination addresses to see if they are the same. However, Bots does not disclose detecting if any group is a subset of any other group. Accordingly, Bots neither teaches nor suggests "discarding said first data packet in response to detecting said first incoming PCS **is not a subset of an interface community set (IFCS)** of said interface" or "discarding said first data packet in response to detecting said outgoing PCS **is not a subset of said destination community set**," as is recited in claim 1.

In light of the foregoing, Applicant submits the application is in condition for allowance, and notice to that effect is respectfully requested. If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above referenced application from becoming abandoned, Applicant hereby petitions for such an extension. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert & Goetzel PC Deposit Account No. 501505/5181-75900/RDR. Also enclosed herewith are the following items:

☒ Notice of Appeal
☒ Fee Authorization

Respectfully submitted,

/Rory D. Rankin/
Reg. No. 47,884
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850
Date: November 14, 2006